

1 The opinion in support of the decision being entered today was *not* written  
2 for publication in and is *not* binding precedent of the Board.

3  
4 UNITED STATES PATENT AND TRADEMARK OFFICE

5  
6  
7 BEFORE THE BOARD OF PATENT APPEALS  
8 AND INTERFERENCES

9  
10  
11 *Ex parte* RAANAN LIEBERMANN

12  
13  
14 Appeal 2007-0215  
15 Application 09/662,451  
16 Technology Center 1700

17  
18  
19 Decided: March 16, 2007

20  
21  
22 Before STUART S. LEVY, LINDA E. HORNER, and ANTON W. FETTING,  
23 *Administrative Patent Judges.*

24 FETTING, *Administrative Patent Judge.*

25 DECISION ON APPEAL

26  
27  
28 STATEMENT OF CASE

29 This appeal involves claims 1-7, 9-64 and 122<sup>1</sup>, the only claims pending in this  
30 application. We have jurisdiction over the appeal pursuant to 35 U.S.C. §§ 6 and  
31 134.

32  
33 We AFFIRM-IN-PART.

\_\_\_\_\_  
<sup>1</sup> Claims 8 and 65-121 are cancelled.

1       The Appellant invented a system to secure personal transactions (Specification  
2   6). An understanding of the invention can be derived from a reading of exemplary  
3   claim 1, which is reproduced below.

- 4       1. A method for carrying out personal transactions comprising:  
5             providing a system for performing said personal transactions;  
6             registering a user of said system;  
7             said registering step comprising said user accessing said system  
8             and providing said system with personal information about said user;  
9             said registering step further comprising selecting an  
10            identification number for said user;  
11            said registering step further comprising creating a PIN number  
12            by selecting a plurality of single digit numbers to act as a first  
13            segment of said PIN number; and  
14            said PIN number creating step further comprising selecting at  
15            least two digits for a security segment to be incorporated into said PIN  
16            number wherein an alarm signal is sent when said user enters said PIN  
17            number with at least one of said at least two digits used for said  
18            security segment.

19  
20       This appeal arises from the Examiner's Final Rejection, mailed November 23,  
21   2005. The Appellant filed a Brief in support of the appeal on April 26, 2006, and  
22   the Examiner mailed an Answer to the Appeal Brief on May 30, 2006. A Reply  
23   Brief was filed on August 3, 2006.

PRIOR ART

The prior art references of record relied upon by the Examiner in rejecting the appealed claims are:

Zingher	US 5,731,575	Mar. 24, 1998
Franklin	US 5,883,810	Mar. 16, 1999
Rogers	US 5,946,386	Aug. 31, 1999
Hoffman	US 6,366,682 B1	Apr. 2, 2002 (Oct. 30, 1998)

REJECTIONS<sup>2</sup>

Claims 1-7, 9, 42-45 and 61 stand rejected under 35 U.S.C. § 103(a) as obvious over Hoffman and Zingher.

Claims 10-17, 25-41, 46-60, 62-64 and 122 stand rejected under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, and Rogers.

Claims 18-24 stand rejected under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, Rogers, and Franklin.

---

<sup>2</sup> The Answer details the rejections as claims 1-7, 9-17, 35-36, 42-45, and 61 over Hoffman and Zingher; 25-34, 37-41, 46-60, 62-64 and 122 over Hoffman, Zingher, and Rogers; and 18-24 over Hoffman, Zingher, and Franklin. However, this characterization is technically inaccurate because claim 122, from which claims 10-41 depend, includes Rogers in its rejection. Both the Examiner's and the Appellant's arguments are consistent with the application of the art indicated above, in which all claims depending from claim 122 also include Rogers in their rejections, and so therefore, the rejections are treated as such.

1 The Examiner applies Zingher to show the use of Personal Identification  
2 Number (PIN) digits adapted for use to trigger an alarm for use under duress;  
3 Hoffman to show implementation details of PIN systems, Franklin for  
4 implementation details of purchase transactions that might use PIN's; and Rogers  
5 to show evidence that system centers that control PIN access would also have  
6 facilities such as e-mail, facsimile and paging communication.

7  
8 ISSUES

9 The issues pertinent to this appeal are

10 *Independent claims 1, 42, and 122 rejected under 35 U.S.C. § 103(a).*

- 11 • Whether the art shows selecting at least two digits for a security segment to  
12 be incorporated into a PIN number wherein an alarm signal is sent when a  
13 user enters that PIN number with at least one of at least two digits used for  
14 the security segment
- 15 • Whether the art, and in particular, regarding claim 42, the combination of  
16 Zingher and Hoffman shows performing e-mail, voice messaging, and  
17 financial transactions
- 18 • Whether there is motivation in the prior art to combine the references

19 *Dependent claims 2-7, 9-17, 21, 22, 35, 36, 43-54 and 61 rejected under 35 U.S.C.*  
20 *§ 103(a).*

- 21 • Whether the art shows or suggests use of a telephone number for a PIN
- 22 • Whether the art shows selecting a digit in said first segment to identify the  
23 location of said second security segment

- 1       • Whether the art shows entering both an identification and PIN number, the  
2       PIN either with or without the security segment, to receive money
- 3       • Whether the art shows inserting a credit card or identification card prior to  
4       entering the identification number (claim 14)
- 5       • Whether the art shows having the user specify an activation time, at least  
6       one monitoring location and at least one assistance preference and calling  
7       the user at that activation time at the monitoring location

8       *Dependent claims 18-20, 23, and 24 rejected under 35 U.S.C. § 103(a).*

- 9       • Whether the art shows downloading information stored in a buffer; opening  
10       a temporary file containing the downloaded information; assigning a  
11       transaction identification number to the temporary file; and transferring the  
12       transaction identification number to the buffer and verifying the transaction  
13       identification number

14       *Dependent claims 25-34, 37-41, 46-60 and 62-64 rejected under 35 U.S.C.*

15                               *§ 103(a).*

- 16       • Whether the art shows providing an electronic box for providing at least one  
17       of an indication of the presence of an e-mail message, the names of the  
18       individual transmitting the e-mail message, and the text of the e-mail  
19       message
- 20       • Whether the art shows triggering a notification signal when said user uses a  
21       particular credit or debit card

22       In particular, the Appellant contends that the art does not show the two digits  
23       for a PIN security segment (Br. 21-23); that neither Hoffman nor Zingher shows  
24       performing e-mail, voice messaging and financial transactions (Br. 23-24); that

1 there is no motivation to combine Rogers's call center with Hoffman or Zingher  
2 (Br. 24-26); that the art fails to show use of a telephone number for a PIN (Br. 27);  
3 that the art fails to show selecting a digit in said first segment to identify the  
4 location of said second security segment (Br. 27); that the art fails to show  
5 entering both an identification and PIN number, the PIN either with or without the  
6 security segment, to receive money (Br. 27-29); that the art fails to show inserting  
7 a credit card or identification card prior to entering the identification card (claim  
8 14); that the art fails to show having the user specify an activation time, at least one  
9 monitoring location and at least one assistance preference and calling the user at  
10 that activation time at the monitoring location (Br. 29-30); downloading  
11 information stored in a buffer; opening a temporary file containing the downloaded  
12 information; assigning a transaction identification number to the temporary file;  
13 and transferring the transaction identification number to the buffer and verifying  
14 the transaction identification number (Br. 30-32); there is no reason to apply  
15 Rogers's communications teachings to Hoffman (Br. 32-40); that the art fails to  
16 show providing an electronic box for providing at least one of an indication of the  
17 presence of an e-mail message, the names of the individual transmitting the e-mail  
18 message, and the text of the e-mail message (Br. 36); and that the art fails to show  
19 triggering a notification signal when said user uses a particular credit or debit card  
20 (Br. 37).

## FACTS PERTINENT TO THE ISSUES

21  
22  
23 The following findings of fact (FF) pertinent to the issues in this appeal are  
24 supported by a preponderance of the evidence.

1) Each of the three independent claims, viz. 1, 42, and 122, call for a PIN that has two segments. One segment is comprised of a plurality of selected digits. The other segment is comprised of at least one digit, which, when entered within the PIN entry, triggers an alarm.

2) Claim 1 adds a further limitation that at least two digits are selected for the second segment, however, by the terms of claim 1, entry of at least one of them is sufficient to trigger the alarm.

3) Choosing a second digit that is not used is a nonfunctional statement of intended use relative to the operation of claim 1.

4) A PIN is an authentication code, or as Zingher refers to it (Zingher, col. 1, ll. 49-52), an access code.

5) A PIN authenticates, i.e., grants access to, the person whose identification, either by entry of an identification number, such as an account number, or its equivalent by biometric measurement, has been entered.

6) Entry of an identification number at an ATM or at a merchant's terminal is generally by a card identifying the user and the user's account.

7) Thus, use of a PIN inherently comprises entry of both an identification datum, such as a number, and the PIN. This is evidenced by the Background section of Hoffman (Hoffman, col. 1, ll. 45-60).

8) Zingher describes the use of multiple sets of digits that may be entered when a system is expecting a PIN to be entered. Zingher refers to a set of digits that are entered when PIN entry is expected, but is meant to trigger an alarm as a personal distress number (PDN) (Zingher, col. 2, l. 66- col. 3, l. 11).

9) Thus, each of the numbers characterized as PINs in independent claims 1, 42, and 122, is the functional equivalent of what Zingher refers to as a PDN when the claimed segment with claimed digit is entered that triggers an alarm.

10) Zingher describes several methods for devising a PDN. In particular, Zingher refers to methods involving an altered PIN, particularly

(1) a typical prestored PIN number prestored in the memory banks of the bank computer or on the magnetic strip of the costumer's [sic] card, and (2) an algorithm which may alter the PIN number to achieve a PDN number.

(Zingher, col. 3, ll. 26-29).

In particular, Zingher describes implementations in which

the PIN could be N digits in length and the PDN could be either N-1, N, or N+1 digits. By expanding the range of PIN lengths, the PDN length could also be shortened or lengthened as required. There is no requirement that the extra digit be specifically designated. That is, any digit in the N+1 position could be used to trigger the alarm system. All the customer has to know is to press any extra digit he wants to.

(Zingher, col. 11, ll. 39-46).

11) Thus, Zingher describes selecting any digit, which is one of at least two digits, for a security segment to be incorporated into a PIN number wherein an alarm signal is sent when a user enters that PIN number with at least one of at least two digits used for the security segment.

12) Similarly, Zingher suggests selecting a digit in said first segment (N) to identify the location of said second security segment (N+1).

13) Similarly, Zingher suggests entering both an identification and PIN number, the PIN either with (thus forming Zingher's PDN) or without (thus forming Zingher's PIN) the security segment, to receive money.



1 14) Similarly, the use of a credit card or a bank card at an ATM suggests  
2 inserting a credit card or identification card prior to entering a PIN, although  
3 nothing in the art of record suggests entering both the identification number and  
4 PIN after inserting such a card.

5 15) Rogers describes performing voice messaging, e-mail, Fax, and data  
6 messaging (col. 4, ll. 27-34). Hoffman, Zingher, and Franklin each describe  
7 financial transactions in their background. As to the combined teachings of  
8 Hoffman and Zingher, absent Franklin, in particular, Hoffman describes a terminal  
9 that

10 communicates through a modem 18 with the DPC 1 through  
11 transaction request messages 19 and transaction response messages 20  
12 using one of the interconnecting means in FIG. 1 such as a cable TV  
13 network, cellular telephone network, telephone network, the Internet,  
14 or an X.25 network.

15 (Hoffman, col. 9, ll. 38-43).

16 16) These transaction messages are commonly conveyed via voice messaging, e-  
17 mail, Fax, and data messaging.

18 17) Thus, Zingher and Hoffman in particular, and more generally, those  
19 references coupled with Rogers, show performing e-mail, voice messaging, and  
20 financial transactions.

21 18) Zingher suggests the use of the user's telephone numbers for a PIN or PDN  
22 (Zingher, col. 6, ll. 51-56).

23 19) Thus, Zingher suggests use of a telephone number for a PIN.

24 20) As the Examiner pointed out (Answer 6), Franklin describes the internal  
25 mechanics of using a credit or debit card with a PIN in a commercial transaction

1 where the issuing bank creates a temporary customer account record in the  
2 customer database 64 and assigns a temporary PIN (personal identification  
3 number) or other type of customer identifier to that account.

4 (Franklin, col. 6, ll. 50-54).

5 Of greater pertinence, Franklin later describes, in thorough detail, numerous  
6 instances of downloading information stored in a buffer; opening a temporary file  
7 containing the downloaded information; assigning a transaction identification  
8 number to the temporary file; and transferring the transaction identification number  
9 to the buffer and verifying the transaction identification number in

10 the online commerce system 20 during a transaction phase. This phase  
11 involves the customer 22 engaging in an online commerce transaction  
12 with the merchant 24. As part of the process, the customer 22 requests  
13 a transaction number from the bank 26 to be used in the commerce  
14 transaction. . . .

15 Upon reaching this method of payment field, the customer  
16 clicks the card button UI 54 on the browser toolbar to invoke a card  
17 transaction module 72. . . .

18 Upon clicking the button UI 54, a dialog box appears on the  
19 display to inform the customer that they have requested a secure card  
20 number. The customer is prompted by the dialog box to input a  
21 password for identification purposes. This password might be the  
22 private key (if the customer knows the key value) or it may be a  
23 separate name or number created by the customer. The operating  
24 system 48 checks the password prior to allowing access to the  
25 certificate store 50. If the password is approved, the transaction  
26 module 72 prepares a request for a transaction number, digitally signs  
27 the request using the customer's private key, and submits the signed  
28 request to the issuing bank's computer 32 via the Internet 34 (flow  
29 arrow 2 in FIG. 3). The request contains the certificate originally  
30 issued by the bank.

31 . . . Assuming the signature and request are valid and the customer's  
32 account is in good standing, the account manager 60 instructs the

1 transaction number generator 62 to create a transaction number to be  
2 used as a proxy for the customer account number during the online  
3 commerce transaction. The account manager 60 associates the  
4 transaction number with the customer account number in a data record  
5 on the customer database 64. As a result, the online commerce card  
6 now has two numbers associated therewith: a permanent customer  
7 account number and a transaction number that serves as a proxy for  
8 the customer account number.

9 FIG. 4 shows one exemplary implementation of creating a  
10 transaction number and associating that number with the customer's  
11 account number. A customer record 80 for the requesting customer is  
12 stored in the customer database 64 and contains a customer account  
13 number. Suppose, for example, the customer account number is a 16-  
14 digit credit card number. Credit card numbers comply with a  
15 standardized format having four spaced sets of numbers, as  
16 represented by the number "0000 0000 0000 0000". The first five-to-  
17 seven digits are reserved for processing purposes. It identifies the  
18 issuing bank, the card type, and so forth. The last 16<sup>th</sup> digit is used as a  
19 sum check for the 16-digit number. The intermediary eight-to-ten  
20 digits are used to uniquely identify the customer.

21 The transaction number generator 62 generates a transaction  
22 number for the online commerce card that is formatted identically to  
23 the customer account number. In this example, the number generator  
24 62 creates a 16-digit transaction number having four spaced sets of  
25 numbers, as represented by the number "1111 1111 1111 1111". The  
26 transaction number resembles a credit card number in all respects,  
27 except that the first five-seven-digits are coded by the issuing bank to  
28 identify the number as a fictitious electronic proxy number, rather  
29 than a real credit card number.

30 The account manager 60 associates the temporary transaction  
31 number with the permanent customer account number by relating the  
32 two numbers in a data record 82. More particularly, the account  
33 manager creates data record 82 in a proxy/customer account cross-  
34 reference database. The data record 82 is keyed with the customer  
35 account number to identify the customer record 80. The transaction  
36 number is then written to the data record 82. In this manner, the  
37 customer account record 80 can be cross-referenced via the

1 transaction record 82 using the transaction number as an index. The  
2 issuing bank will use the transaction record 82 at a later time when the  
3 merchant submits the transaction number for payment authorization.

4 . . . The transaction number is valid for only one transaction. For  
5 added security, the transaction number can be linked to transaction  
6 information to ensure that the number is only used for one specific  
7 transaction. The transaction module 72 executing on the customer  
8 computer 28 may require the customer to enter information pertaining  
9 to the purchase, like the purchase price, the model or item number, the  
10 merchant name, and the like. The issuing bank can then tie the  
11 transaction number to this specific transaction data within the  
12 transaction record 82.

13 Once the transaction record 82 is created and related to the  
14 customer record 80, the issuing bank computer 32 sends the  
15 transaction number to the customer computer 28 (flow arrow 3 in FIG.  
16 3). The real customer account number is not sent to the customer, but  
17 is retained at the issuing bank in secrecy. In the credit card case, this  
18 means that the true credit card number is never sent over the Internet  
19 34, thereby eliminating the possibility of interception and illicit use by  
20 a thief.

21 At the customer computer, the transaction number is presented  
22 in a graphical window by the transaction module 72. If the order form  
23 is compatible, the customer can click on an icon to have the number  
24 automatically entered into the merchant order form 70. Otherwise, in a  
25 worst case scenario, the customer manually enters the proxy  
26 transaction number into the merchant's HTML order form 70. Since  
27 the transaction number has the identical 16-digit format as a real  
28 credit card number, the customer enters the 16-digit number as if it  
29 were his/her real credit card number.

30 The user may also be required to enter an expiration date, which  
31 may or may not be sent from the issuing bank. Essentially, the  
32 expiration date can be any future date that is not too far in the distant  
33 future, such as less than two to three years. The customer then submits  
34 the completed order form 70 over the Internet 34 to the merchant  
35 computer 30.

36 Authorization Phase

1           FIG. 5 shows the online commerce system 20 during a payment  
2 authorization phase. This phase involves the merchant 24 seeking  
3 authorization from the issuing bank 26 to honor the customer's  
4 transaction number received by the merchant in the commerce  
5 transaction with the customer. The information exchange between the  
6 merchant computer 30 and the bank computer 32 during the  
7 authorization phase are illustrated as enumerated lines.

8           The merchant 30 receives the transaction number from the  
9 Internet and processes the transaction number using its existing  
10 computer system. There is no software components added to the  
11 merchant computer as part of the online commerce system 20. Rather,  
12 the merchant computer 30 treats the transaction number of the online  
13 commerce card no differently than it treats a standard credit card  
14 number. In fact, the merchant computer 30 most likely will not be able  
15 to distinguish between the two types of numbers.

16           In FIG. 5, the merchant computer submits a request for  
17 authorization over a payment network 36 to the bank computing  
18 center 32 (flow arrow 1 in FIG. 5). This illustration is simplified for  
19 discussion purposes, as other participants will most likely be involved.  
20 For instance, the merchant computer 30 typically submits the request  
21 for authorization to its acquiring bank (not shown) by conventional  
22 means. The acquiring bank validates the authorization request by  
23 verifying that the merchant is a valid merchant and that the credit card  
24 number represents a valid number. The acquiring bank then forwards  
25 the authorization request to the issuing bank. The routing to the  
26 issuing bank via the payment network is handled through  
27 conventional techniques.

28           When the bank computer 32 receives the authorization request,  
29 it first examines the transaction number to determine whether it is a  
30 valid number. A transaction number identifier 90 executing at the  
31 bank computer 32 examines all incoming account numbers to  
32 segregate proxy transaction numbers from real credit card numbers.  
33 On a daily basis, it is likely for the bank computer 32 to handle many  
34 account numbers on the order of tens or hundreds of thousands. Most  
35 of the numbers are expected to be real credit card account numbers.  
36 Only a small percentage is anticipated to be temporary transaction  
37 numbers. The transaction number identifier 90 filters out authorization

1 requests that pertain to transaction numbers from authorization request  
2 that pertain to real customer account numbers. In the continuing  
3 example, the transaction number identifier 90 recognizes the number  
4 submitted by the merchant computer 30 as a transaction number based  
5 on the first five-to-seven digits.

6 The transaction number identifier 90 passes the transaction  
7 number to the account manager 60. The account manager 60 uses the  
8 transaction number as an index to transaction records in the customer  
9 database 64. If no records are found, the number is deemed invalid  
10 and the bank computer 32 returns a message disapproving the  
11 transaction to the merchant computer 30. If a record is found, the  
12 account manager 60 examines any extra transaction information, such  
13 as purchase amount and merchant ID, which is typically included in  
14 the authorization request to double check the accuracy of the request.

15 Once a valid transaction record 82 is located, the account  
16 manager 60 cross-references to the associated customer account  
17 number and uses this number to index the customer record 80. The  
18 account manager 60 substitutes the customer account number in place  
19 of the transaction number in the merchant authorization request. The  
20 account manager 60 then submits the authorization request to the  
21 bank's traditional processing system 92 for normal authorization  
22 processing (e.g., confirm account status, credit rating, credit line, etc.).

23 After the request is processed, the processing system 92 returns  
24 an authorization response to the account manager 60. The account  
25 manager fetches the transaction number from the cross-referenced  
26 data records 80 and 82 in the database 64 and substitutes the  
27 transaction number in place of the customer account number in the  
28 bank's authorization reply. The bank computing center 32 then returns  
29 the authorization reply to the merchant computer 30 via the payment  
30 network 36 (flow arrow 2 in FIG. 5).

31 (Franklin, col. 8, l. 15 – col. 11, l. 40).

32 Similarly, Hoffman describes an internet point of sale terminal (IPT), in which

33 [i]n addition to identifying the buyer, the IPT must also identify the  
34 remote seller who is the counterparty to the transaction. The seller  
35 must also identify both the DPC [data processing center] and the IPT.

1           The Internet Shopper program stores the hostname (or other  
2           form of net name) of the seller from which the purchase is taking  
3           place so that the DPC can verify the seller's identity. . . .

4           First, the IPT connects to the seller using the Internet. . . .

5           Once connected, the IPT downloads the seller identification  
6           code, and both price and product information from the seller. Once the  
7           buyer is ready to make a purchase, he selects the merchandise he  
8           wishes to buy. Then, the buyer enters the biometric-PIN using the  
9           BIA/PC [biometric input apparatus / personal computer], the IPT  
10          sends the seller identification code, the product identification  
11          information, and the amount to the BIA, and instructs it to construct a  
12          Remote Commercial Transaction Message. Then the IPT sends the  
13          request to the seller via the secure channel.

14          . . . The DPC validates the biometric-PIN, cross-checks the seller  
15          identification code contained in the request with the seller  
16          identification code stored under the hostname that was sent in the  
17          request, and then sends a transaction to the credit/debit network. Once  
18          the credit/debit network responds, the DPC constructs a response  
19          message including the credit/debit authorization, an encrypted private  
20          code, and the address of the buyer, and sends that message back to the  
21          seller.

22          Once the seller receives the response, it copies the buyer's  
23          mailing address out of the response, makes note of the authorization  
24          code, and forwards the response message to the IPT.

25          (Hoffman, col. 15, l. 44 – col. 16, l. 27).

26   21)   Thus both Franklin and Hoffman describe the act of creating a temporary  
27   record including downloaded purchaser identification and PIN and seller  
28   identification information stored in a buffer; opening a temporary file containing  
29   the downloaded information; assigning a transaction identification number to the  
30   temporary file; and transferring the transaction identification number to the buffer  
31   and verifying the transaction identification number to create a Remote Commercial  
32   Transaction Message.

22) Rogers describes providing an electronic box in fig. 6c for providing all of, and therefore at least one of, an indication of the presence of an e-mail message, the names of the individual transmitting the e-mail message, and the text of the e-mail message.

23) Credit card issuers have triggered notification signals in the form of monthly statements since the inception of credit cards. The notification signal of each use was added to the database for the monthly billings whenever a particular credit card was used. On-line banking software, suggested by the on-line commerce transactions of Franklin, are notoriously old and well known to have triggered an electronic notification signal whenever a user used a particular credit or debit card since at least as far back as the introduction of Quicken 98 in 1998.

24) Zingher provides implementation details for securing the PIN taught by Hoffman.

25) Franklin provides implementation details for how the transactions described by Hoffman are executed.

26) Rogers provides an exemplary environment in which Zingher's security over PINs may be needed with Rogers's security code (Rogers, col. 44, ll. 1-4). Rogers also describes its call center operations as a mechanism for handling business communications (Rogers, col. 1, ll. 42-47).

27) Both Franklin and Hoffman describe financial transactions that are conveyed via the conduits of business communications, which Rogers provides more efficient and effective operations over.

28) Thus, it would have been obvious to a person of ordinary skill in the art to have applied the teachings of Zingher and Franklin to Hoffman to find



1 implementation details and to have applied Rogers to Hoffman for greater  
2 efficiency in Hoffman's operations.

3 ANALYSIS

4 *Claims 1-7, 9, 42-45 and 61 rejected under 35 U.S.C. § 103(a) as obvious over*  
5 *Hoffman and Zingher*

6 *and*

7 *Claims 10-17, 25-41, 46-60, 62-64 and 122 rejected under 35 U.S.C. § 103(a) as*  
8 *obvious over Hoffman, Zingher, and Rogers.*

9 The above findings of fact demonstrate that

- 10 • The art shows selecting at least two digits for a security segment to be  
11 incorporated into a PIN number wherein an alarm signal is sent when a user  
12 enters that PIN number with at least one of at least two digits used for the  
13 security segment (FF 11).
- 14 • The art, and in particular, regarding claim 42, the combination of Zingher  
15 and Hoffman, coupled with Rogers, shows performing e-mail, voice  
16 messaging and financial transactions (FF 17).
- 17 • It would have been obvious to a person of ordinary skill in the art to have  
18 applied the teachings of Zingher to Hoffman to find implementation details  
19 and to have applied Rogers to Hoffman for greater efficiency in Hoffman's  
20 operations (FF 28).
- 21 • The art shows or suggests use of telephone number for a PIN (FF 19).
- 22 • The art shows selecting a digit in said first segment to identify the location  
23 of said second security segment (FF 12)

- 1       • The art shows entering both an identification and PIN number, the PIN  
2       either with or without the security segment, to receive money (FF13)
- 3       • The art shows inserting a credit card or identification card prior to entering a  
4       PIN, but not prior to entering both the identification number and PIN (claim  
5       14) (FF 14).

6       Further, the art does not show having the user specify an activation time, at  
7       least one monitoring location, and at least one assistance preference and calling the  
8       user at that activation time at the monitoring location of claims 35 and 36, nor has  
9       the Examiner pointed to anywhere in the art of record that this subject matter is  
10      described.

11      Thus, the Examiner has shown by a preponderance of substantial evidence that  
12      the claim limitations of claims 1-7, 9-13, 15-17, 25-34, 37-64 and 122 are found in  
13      or suggested by the art and that it would have been obvious to a person of ordinary  
14      skill in the art to have combined the respective teachings. Accordingly we sustain  
15      the Examiner's rejection of claims 1-7, 9, 42-45 and 61 under 35 U.S.C. § 103(a) as  
16      obvious over Hoffman and Zingher and we sustain the Examiner's rejection of  
17      claims 10-13, 15-17, 25-34, 37-41, 46-60, 62-64 and 122, but do not sustain the  
18      rejection of claims 14, 35, and 36, under 35 U.S.C. § 103(a) as obvious over  
19      Hoffman, Zingher, and Rogers.

20

21           *Claims 18-24 rejected under 35 U.S.C. § 103(a) as obvious over Hoffman,*  
22                                   *Zingher, Rogers, and Franklin.*

23      The above findings of fact demonstrate that

- 1       • The art shows downloading information stored in a buffer; opening a  
2       temporary file containing the downloaded information; assigning a  
3       transaction identification number to the temporary file; and transferring the  
4       transaction identification number to the buffer and verifying the transaction  
5       identification number (FF 21).
- 6       • The art shows providing an electronic box for providing at least one of an  
7       indication of the presence of an e-mail message, the names of the individual  
8       transmitting the e-mail message, and the text of the e-mail message (FF 22).
- 9       • The art shows triggering a notification signal when said user uses a  
10      particular credit or debit card (FF 23).
- 11      • It would have been obvious to a person of ordinary skill in the art to have  
12      applied the teachings of Zingher and Franklin to Hoffman to find  
13      implementation details and to have applied Rogers to Hoffman for greater  
14      efficiency in Hoffman's operations (FF 28).

15

16       The Appellant argued that the Examiner improperly rejected claims 21 and 22  
17      on the technical basis that their rejection did not include the same art as their parent  
18      claim 20 (Br. 29), which the Examiner noted and corrected (Answer 2-3). The  
19      Appellant did not recite any argument in the Reply Brief regarding patentability of  
20      claim 21 and 22, but only commented that they did not see the Examiner pointing  
21      out the analysis for their patentability (Reply Br. 5-6). Our reviewing court has  
22      recently held that, while it is correct that each claim must be considered separately,  
23      where the dispositive issue, in this case using a PIN with a security segment and a  
24      transaction identifier in a transaction, has been considered, and its analysis set forth

1 elsewhere in the opinion, failure to set forth this analysis separately for each  
2 affected claim on a claim by claim basis does not represent reversible error. *Hakim*  
3 *v Cannon Avent Group*, No. 2005-1398, slip op. (Fed. Cir., Feb. 23, 2007).  
4 Certainly the limitations added by claims 21 and 22 of debiting and crediting  
5 accounts for purchases have been inherent to purchases for a notoriously old  
6 duration, essentially having existed at least since Luca Pacioli first codified double  
7 entry accounting in 1494, and are therefore of minimal weight in terms of  
8 patentability analysis.

9 Thus, the Examiner has shown by a preponderance of substantial evidence that  
10 the claim limitations of claims 18-24 are found in or suggested by the art and that it  
11 would have been obvious to a person of ordinary skill in the art to have combined  
12 the respective teachings. Accordingly we sustain the Examiner's rejection of  
13 claims 18-24 under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, Rogers  
14 and Franklin.

## 15 16 DECISION

17 To summarize, our decision is as follows:

- 18 • The rejection of claims 1-7, 9, 42-45 and 61 under 35 U.S.C. § 103(a) as  
19 obvious over Hoffman and Zingher is *sustained*.
- 20 • The rejection of claims 10-13, 15-17, 25-41, 46-60, 62-64 and 122 under 35  
21 U.S.C. § 103(a) as obvious over Hoffman, Zingher, and Rogers is *sustained*.
- 22 • The rejection of claims 14, 35-36 under 35 U.S.C. § 103(a) as obvious over  
23 Hoffman, Zingher, and Rogers is *not sustained*.

- The rejection of claims 18-24 under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, Rogers, and Franklin is *sustained*.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a) (2006).

AFFIRMED-IN-PART

hh

Barry L Kelmachter  
Bachman & LaPointe PC  
Suite 1201  
900 Chapel Street  
New Haven, CT 06510-2802